

ORP.3.A8 Messung und Auswertung des Lernerfolgs (S) [Personalabteilung]

Die Lernerfolge im Bereich Informationssicherheit SOLLTEN zielgruppenbezogen gemessen und ausgewertet werden, um festzustellen, inwieweit die in den Sensibilisierungs- und Schulungsprogrammen zur Informationssicherheit beschriebenen Ziele erreicht sind. Die Messungen SOLLTEN sowohl quantitative als auch qualitative Aspekte der Sensibilisierungs- und Schulungsprogramme zur Informationssicherheit berücksichtigen. Die Ergebnisse SOLLTEN bei der Verbesserung des Sensibilisierungs- und Schulungsangebots zur Informationssicherheit in geeigneter Weise einfließen.

Der oder die Informationssicherheitsbeauftragte SOLLTE sich regelmäßig mit der Personalabteilung und den anderen für die Sicherheit relevanten Ansprechpartnern (Datenschutz, Gesundheits- und Arbeitsschutz, Brandschutz etc.) über die Effizienz der Aus- und Weiterbildung austauschen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

ORP.3.A9 Spezielle Schulung von exponierten Personen und Institutionen (H)

Besonders exponierte Personen SOLLTEN vertiefende Schulungen in Hinblick auf mögliche Gefährdungen sowie geeignete Verhaltensweisen und Vorsichtsmaßnahmen erhalten.

4. Weiterführende Informationen**4.1. Wissenswertes**

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 im Kapitel 7.2 Vorgaben für die Sensibilisierung und Schulung von Beschäftigten.

Das Information Security Forum (ISF) definiert in seinem Standard „The Standard of Good Practice for Information Security“ unter PM2 verschiedene Anforderungen an Sensibilisierung und Schulung von Beschäftigten.

Das BSI bietet unter <https://www.bsi.bund.de/grundschutzkurs> einen Online-Kurs zum IT-Grundschutz an, der die Methodik des IT-Grundschutzes vorstellt.

Das BSI bietet ein zweistufiges Schulungskonzept zum Thema IT-Grundschutz an. Bei dem Schulungskonzept kann man einen Nachweis eines IT-Grundschutz-Praktikers erwerben und sich weiter zum IT-Grundschutz-Berater vom BSI zertifizieren lassen.

Eine Liste der Schulungsanbieter, die die BSI Schulung zum IT-Grundschutz-Praktiker und IT-Grundschutz-Berater anbieten, ist unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/Personenzertifizierung-IT-Grundschutzberater/Schulungen-zum-IT-Grundschutz-Praktiker-und-IT-Grundschutzberater/schulungen-zum-it-grundschutz-praktiker-und-it-grundschutzberater_node.html zu finden.



ORP.4 Identitäts- und Berechtigungsmanagement

1. Beschreibung

1.1. Einleitung

Der Zugang zu schützenswerten Ressourcen einer Institution ist auf berechnigte Benutzende und berechnigte IT-Komponenten einzuschränken. Benutzende und IT-Komponenten müssen zweifelsfrei identifiziert und authentifiziert werden. Die Verwaltung der dafür notwendigen Informationen wird als Identitätsmanagement bezeichnet.

Beim Berechnigungsmanagement geht es darum, ob und wie Benutzende oder IT-Komponenten auf Informationen oder Dienste zugreifen und diese benutzen dürfen, ihnen also basierend auf ihren Rechten Zutritt, Zugang oder Zugriff zu gewähren oder zu verweigern ist. Berechnigungsmanagement bezeichnet die Prozesse, die für Zuweisung, Entzug und Kontrolle der Rechte erforderlich sind.

Die Übergänge zwischen den beiden Begriffen sind fließend, daher wird in diesem Baustein der Begriff Identitäts- und Berechnigungsmanagement (englisch Identity and Access Management, IAM) benutzt. Zur besseren Verständlichkeit wird in diesem Baustein der Begriff „Benutzendenkennung“ bzw. „Kennung“ synonym für „Benutzendenkonto“, „Konto“, „Login“ und „Account“ verwendet. In diesem Baustein wird der Begriff „Passwort“ als allgemeine Bezeichnung für „Passphrase“, „PIN“ oder „Kennwort“ verwendet.

1.2. Zielsetzung

Ziel des Bausteins ist es, dass Benutzende oder auch IT-Komponenten ausschließlich auf die IT-Ressourcen und Informationen zugreifen können, die sie für ihre Arbeit benötigen und für die sie autorisiert sind, und unautorisierten Benutzenden oder IT-Komponenten den Zugriff zu verwehren. Dazu werden Anforderungen formuliert, mit denen Institutionen ein sicheres Identitäts- und Berechnigungsmanagement aufbauen sollten.

1.3. Abgrenzung und Modellierung

Der Baustein ORP.4 *Identitäts- und Berechnigungsmanagement* ist für den Informationsverbund einmal anzuwenden.

In diesem Baustein werden grundsätzliche Anforderungen für den Aufbau eines Identitäts- und Berechnigungsmanagements beschrieben.

Anforderungen, die Komponenten eines Identitäts- und Berechnigungsmanagement betreffen, wie Betriebssysteme oder Verzeichnisdienste, sind in den entsprechenden Bausteinen zu finden (z. B. SYS.1.3 *Server unter Linux und Unix*, SYS.1.2.3 *Windows Server*, APP.2.1 *Allgemeiner Verzeichnisdienst*, APP.2.2 *Active Directory Domain Services*).

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein ORP.4 *Identitäts- und Berechnigungsmanagement* von besonderer Bedeutung.

2.1. Fehlende oder unzureichende Prozesse beim Identitäts- und Berechnigungsmanagement

Sind Prozesse beim Identitäts- und Berechnigungsmanagement unzureichend definiert oder implementiert, ist nicht gewährleistet, dass Zugriffe auf das erforderliche Maß eingeschränkt sind und so gegen die Prinzipien Need-to-

Know bzw. Least-Privilege verstoßen wird. Der IT-Betrieb erhält möglicherweise keine Informationen über personelle Veränderungen, so dass beispielsweise Konten von ausgeschiedenen Mitarbeitenden nicht gelöscht werden. Diese können somit weiterhin auf schützenswerte Informationen zugreifen.

Auch ist es möglich, dass Mitarbeitende, die in eine neue Abteilung versetzt wurden, ihre alten Berechtigungen behalten und dadurch mit der Zeit umfangreiche Gesamtberechtigungen ansammeln.

2.2. Fehlende zentrale Deaktivierungsmöglichkeit von Konten

In Institutionen haben Mitarbeitende oft Konten für diversen IT-Systemen, wie Produktiv-, Test-, Qualitätssicherungs- oder Projekt-Systeme. Diese befinden sich meist in unterschiedlichen Zuständigkeitsbereichen und werden oft von unterschiedlichen Administrierenden verwaltet. Das führt unter Umständen dazu, dass nicht auf allen IT-Systemen eine gleiche und eindeutige Kennung verwendet wird und es auch keine zentrale Übersicht über die Konten auf den einzelnen IT-Systemen gibt. In einem solchen Szenario ist es nicht möglich, bei einem Angriff oder einem Passwortdiebstahl in einem Arbeitsschritt alle Konten der betroffenen Mitarbeitenden zu deaktivieren. Auch können in diesem Szenario bei Ausscheiden von Mitarbeitenden aus der Institution nicht in einem Arbeitsschritt alle Zugänge gesperrt werden.

2.3. Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten

Wenn die Vergabe von Zutritts-, Zugangs- und Zugriffsrechten schlecht geregelt ist, führt das schnell zu gravierenden Sicherheitslücken, z. B. durch Wildwuchs in der Rechtevergabe. Bei der Einführung von Identitätsmanagement-Systemen oder Revisionen stellt sich häufig heraus, dass verschiedene Personen in unterschiedlichsten Organisationseinheiten für die Vergabe von Berechtigungen zuständig sind. Dies führt unter Umständen dazu, dass Benutzende Berechtigungen auf Zuruf erhalten oder umgekehrt nur über unnötig komplizierte Wege an diese kommen. Dadurch können einerseits fehlende Berechtigungen die tägliche Arbeit behindern, andererseits können so Berechtigungen ohne Erfordernis vergeben werden und so ein Sicherheitsrisiko darstellen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins ORP.4 *Identitäts- und Berechtigungsmanagement* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Informationssicherheitsbeauftragte (ISB)
Weitere Zuständigkeiten	Benutzende, IT-Betrieb

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

ORP.4.A1 Regelung für die Einrichtung und Löschung von Benutzenden und Benutzendengruppen (B) [IT-Betrieb]

Es MUSS geregelt werden, wie Benutzendenkennungen und -gruppen einzurichten und zu löschen sind. Jede Benutzendenkennung MUSS eindeutig einer Person zugeordnet werden können. Benutzendenkennungen, die längere Zeit inaktiv sind, SOLLTEN deaktiviert werden. Alle Benutzenden und Benutzendengruppen DÜRFEN NUR über separate administrative Rollen eingerichtet und gelöscht werden. Nicht benötigte Benutzendenkennungen, wie

z. B. standardmäßig eingerichtete Gastkonten oder Standard-Administrierendenkennungen, MÜSSEN geeignet deaktiviert oder gelöscht werden.

ORP.4.A2 Einrichtung, Änderung und Entzug von Berechtigungen (B) [IT-Betrieb]

Benutzendenkennungen und Berechtigungen DÜRFEN NUR aufgrund des tatsächlichen Bedarfs und der Notwendigkeit zur Aufgabenerfüllung vergeben werden (Prinzip der geringsten Berechtigungen, englisch Least Privileges und Erforderlichkeitsprinzip, englisch Need-to-know). Bei personellen Veränderungen MÜSSEN die nicht mehr benötigten Benutzendenkennungen und Berechtigungen entfernt werden. Beantragen Mitarbeitende Berechtigungen, die über den Standard hinausgehen, DÜRFEN diese NUR nach zusätzlicher Begründung und Prüfung vergeben werden. Zugriffsberechtigungen auf Systemverzeichnisse und -dateien SOLLTEN restriktiv eingeschränkt werden. Alle Berechtigungen MÜSSEN über separate administrative Rollen eingerichtet werden.

ORP.4.A3 Dokumentation der Benutzendenkennungen und Rechteprofile (B) [IT-Betrieb]

Es MUSS dokumentiert werden, welche Benutzendenkennungen, angelegte Benutzendengruppen und Rechteprofile zugelassen und angelegt wurden. Die Dokumentation der zugelassenen Benutzendenkennungen, angelegten Benutzendengruppen und Rechteprofile MUSS regelmäßig daraufhin überprüft werden, ob sie den tatsächlichen Stand der Rechtevergabe widerspiegelt. Dabei MUSS auch geprüft werden, ob die Rechtevergabe noch den Sicherheitsanforderungen und den aktuellen Aufgaben der Benutzenden entspricht. Die Dokumentation MUSS vor unberechtigtem Zugriff geschützt werden. Sofern sie in elektronischer Form erfolgt, SOLLTE sie in das Datensicherungsverfahren einbezogen werden.

ORP.4.A4 Aufgabenverteilung und Funktionstrennung (B) [IT-Betrieb]

Die von der Institution definierten unvereinbaren Aufgaben und Funktionen (siehe Baustein ORP.1 *Organisation*) MÜSSEN durch das Identitäts- und Berechtigungsmanagement getrennt werden.

ORP.4.A5 Vergabe von Zutrittsberechtigungen (B) [IT-Betrieb]

Es MUSS festgelegt werden, welche Zutrittsberechtigungen an welche Personen im Rahmen ihrer Funktion vergeben bzw. ihnen entzogen werden. Die Ausgabe bzw. der Entzug von verwendeten Zutrittsmitteln wie Chipkarten MUSS dokumentiert werden. Wenn Zutrittsmittel kompromittiert wurden, MÜSSEN sie ausgewechselt werden. Die Zutrittsberechtigten SOLLTEN für den korrekten Umgang mit den Zutrittsmitteln geschult werden. Bei längeren Abwesenheiten SOLLTEN berechnete Personen vorübergehend gesperrt werden.

ORP.4.A6 Vergabe von Zugangsberechtigungen (B) [IT-Betrieb]

Es MUSS festgelegt werden, welche Zugangsberechtigungen an welche Personen im Rahmen ihrer Funktion vergeben bzw. ihnen entzogen werden. Werden Zugangsmittel wie Chipkarten verwendet, so MUSS die Ausgabe bzw. der Entzug dokumentiert werden. Wenn Zugangsmittel kompromittiert wurden, MÜSSEN sie ausgewechselt werden. Die Zugangsberechtigten SOLLTEN für den korrekten Umgang mit den Zugangsmitteln geschult werden. Bei längeren Abwesenheiten SOLLTEN berechnete Personen vorübergehend gesperrt werden.

ORP.4.A7 Vergabe von Zugriffsrechten (B) [IT-Betrieb]

Es MUSS festgelegt werden, welche Zugriffsrechte an welche Personen im Rahmen ihrer Funktion vergeben bzw. ihnen entzogen werden. Werden im Rahmen der Zugriffskontrolle Chipkarten oder Token verwendet, so MUSS die Ausgabe bzw. der Entzug dokumentiert werden. Die Anwendenden SOLLTEN für den korrekten Umgang mit Chipkarten oder Token geschult werden. Bei längeren Abwesenheiten SOLLTEN berechnete Personen vorübergehend gesperrt werden.

ORP.4.A8 Regelung des Passwortgebrauchs (B) [Benutzende, IT-Betrieb]

Die Institution MUSS den Passwortgebrauch verbindlich regeln (siehe auch ORP.4.A22 *Regelung zur Passwortqualität* und ORP.4.A23 *Regelung für passwortverarbeitende Anwendungen und IT-Systeme*). Dabei MUSS geprüft werden, ob Passwörter als alleiniges Authentisierungsverfahren eingesetzt werden sollen, oder ob andere Authentisierungsmerkmale bzw. -verfahren zusätzlich zu oder anstelle von Passwörtern verwendet werden können.

Passwörter DÜRFEN NICHT mehrfach verwendet werden. Für jedes IT-System bzw. jede Anwendung MUSS ein eigenständiges Passwort verwendet werden. Passwörter, die leicht zu erraten sind oder in gängigen Passwortlisten geführt werden, DÜRFEN NICHT verwendet werden. Passwörter MÜSSEN geheim gehalten werden. Sie DÜRFEN

NUR den Benutzenden persönlich bekannt sein. Passwörter DÜRFEN NUR unbeobachtet eingegeben werden. Passwörter DÜRFEN NICHT auf programmierbaren Funktionstasten von Tastaturen oder Mäusen gespeichert werden. Ein Passwort DARF NUR für eine Hinterlegung für einen Notfall schriftlich fixiert werden. Es MUSS dann sicher aufbewahrt werden. Die Nutzung eines Passwort-Managers SOLLTE geprüft werden. Bei Passwort-Managern mit Funktionen oder Plug-ins, mit denen Passwörter über Onlinedienste Dritter synchronisiert oder anderweitig an Dritte übertragen werden, MÜSSEN diese Funktionen und Plug-ins deaktiviert werden. Ein Passwort MUSS gewechselt werden, wenn es unautorisierten Personen bekannt geworden ist oder der Verdacht dazu besteht.

ORP.4.A9 Identifikation und Authentisierung (B) [IT-Betrieb]

Der Zugriff auf alle IT-Systeme und Dienste MUSS durch eine angemessene Identifikation und Authentisierung der zugreifenden Benutzenden, Dienste oder IT-Systeme abgesichert sein. Vorkonfigurierte Authentisierungsmittel MÜSSEN vor dem produktiven Einsatz geändert werden.

ORP.4.A22 Regelung zur Passwortqualität (B) [IT-Betrieb]

In Abhängigkeit von Einsatzzweck und Schutzbedarf MÜSSEN sichere Passwörter geeigneter Qualität gewählt werden. Das Passwort MUSS so komplex sein, dass es nicht leicht zu erraten ist. Das Passwort DARF NICHT zu kompliziert sein, damit Benutzende in der Lage sind, das Passwort mit vertretbarem Aufwand regelmäßig zu verwenden.

ORP.4.A23 Regelung für passwortverarbeitende Anwendungen und IT-Systeme (B) [IT-Betrieb]

IT-Systeme oder Anwendungen SOLLTEN nur mit einem validen Grund zum Wechsel des Passworts auffordern. Reine zeitgesteuerte Wechsel SOLLTEN vermieden werden. Es MÜSSEN Maßnahmen ergriffen werden, um die Kompromittierung von Passwörtern zu erkennen. Ist dies nicht möglich, so SOLLTE geprüft werden, ob die Nachteile eines zeitgesteuerten Passwortwechsels in Kauf genommen werden können und Passwörter in gewissen Abständen gewechselt werden.

Standardpasswörter MÜSSEN durch ausreichend starke Passwörter ersetzt werden. Vordefinierte Kennungen MÜSSEN geändert werden. Es SOLLTE sichergestellt werden, dass die mögliche Passwortlänge auch im vollen Umfang von verarbeitenden IT-Systemen geprüft wird. Nach einem Passwortwechsel DÜRFEN alte Passwörter NICHT mehr genutzt werden. Passwörter MÜSSEN so sicher wie möglich gespeichert werden. Bei Kennungen für technische Konten, Dienstkonten, Schnittstellen oder Vergleichbares SOLLTE ein Passwortwechsel sorgfältig geplant und gegebenenfalls mit den Anwendungsverantwortlichen abgestimmt werden.

Bei der Authentisierung in vernetzten Systemen DÜRFEN Passwörter NICHT unverschlüsselt über unsichere Netze übertragen werden. Wenn Passwörter in einem Intranet übertragen werden, SOLLTEN sie verschlüsselt werden. Bei erfolglosen Anmeldeversuchen SOLLTEN die passwortverarbeitenden Anwendungen oder die IT-Systeme keinen Hinweis darauf geben, ob Passwort oder Kennung falsch sind.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

ORP.4.A10 Schutz von Benutzendenkennungen mit weitreichenden Berechtigungen (S) [IT-Betrieb]

Benutzendenkennungen mit weitreichenden Berechtigungen SOLLTEN mit einer Mehr-Faktor-Authentisierung, z. B. mit kryptografischen Zertifikaten, Chipkarten oder Token, geschützt werden.

ORP.4.A11 Zurücksetzen von Passwörtern (S) [IT-Betrieb]

Für das Zurücksetzen von Passwörtern SOLLTE ein angemessenes sicheres Verfahren definiert und umgesetzt werden. Die Mitarbeitenden des IT-Betriebs, die Passwörter zurücksetzen können, SOLLTEN entsprechend geschult werden. Bei höherem Schutzbedarf des Passwortes SOLLTE eine Strategie definiert werden, falls Mitarbeitende des IT-Betriebs aufgrund fehlender sicherer Möglichkeiten der Übermittlung des Passwortes die Verantwortung nicht übernehmen können.

ORP.4.A12 Entwicklung eines Authentisierungskonzeptes für IT-Systeme und Anwendungen (S) [IT-Betrieb]

Es SOLLTE ein Authentisierungskonzept erstellt werden. Darin SOLLTE für jedes IT-System und jede Anwendung definiert werden, welche Funktions- und Sicherheitsanforderungen an die Authentisierung gestellt werden. Authenti-

sierungsinformationen MÜSSEN kryptografisch sicher gespeichert werden. Authentisierungsinformationen DÜRFEN NICHT unverschlüsselt über unsichere Netze übertragen werden.

ORP.4.A13 Geeignete Auswahl von Authentisierungsmechanismen (S) [IT-Betrieb]

Es SOLLTEN dem Schutzbedarf angemessene Identifikations- und Authentisierungsmechanismen verwendet werden. Authentisierungsdaten SOLLTEN durch das IT-System bzw. die IT-Anwendungen bei der Verarbeitung jederzeit gegen Ausspähung, Veränderung und Zerstörung geschützt werden. Das IT-System bzw. die IT-Anwendung SOLLTE nach jedem erfolglosen Authentisierungsversuch weitere Anmeldeversuche zunehmend verzögern (Time Delay). Die Gesamtdauer eines Anmeldeversuchs SOLLTE begrenzt werden können. Nach Überschreitung der vorgegebenen Anzahl erfolgloser Authentisierungsversuche SOLLTE das IT-System bzw. die IT-Anwendung die Benutzendenkennung sperren.

ORP.4.A14 Kontrolle der Wirksamkeit der Benutzendentrennung am IT-System bzw. an der Anwendung (S) [IT-Betrieb]

In angemessenen Zeitabständen SOLLTE überprüft werden, ob die Benutzenden von IT-Systemen bzw. Anwendungen sich regelmäßig nach Aufgabenerfüllung abmelden. Ebenso SOLLTE kontrolliert werden, dass nicht mehrere Benutzende unter der gleichen Kennung arbeiten.

ORP.4.A15 Vorgehensweise und Konzeption der Prozesse beim Identitäts- und Berechtigungsmanagement (S) [IT-Betrieb]

Für das Identitäts- und Berechtigungsmanagement SOLLTEN folgenden Prozesse definiert und umgesetzt werden:

- Richtlinien verwalten,
- Identitätsprofile verwalten,
- Benutzendenkennungen verwalten,
- Berechtigungsprofile verwalten sowie
- Rollen verwalten.

ORP.4.A16 Richtlinien für die Zugriffs- und Zugangskontrolle (S) [IT-Betrieb]

Es SOLLTE eine Richtlinie für die Zugriffs- und Zugangskontrolle von IT-Systemen, IT-Komponenten und Datennetzen erstellt werden. Es SOLLTEN Standard-Rechteprofile benutzt werden, die den Funktionen und Aufgaben der Mitarbeitenden entsprechen. Für jedes IT-System und jede IT-Anwendung SOLLTE eine schriftliche Zugriffsregelung existieren.

ORP.4.A17 Geeignete Auswahl von Identitäts- und Berechtigungsmanagement-Systemen (S) [IT-Betrieb]

Beim Einsatz eines Identitäts- und Berechtigungsmanagement-Systems SOLLTE dieses für die Institution und deren jeweilige Geschäftsprozesse, Organisationsstrukturen und Abläufe sowie deren Schutzbedarf geeignet sein. Das Identitäts- und Berechtigungsmanagement-System SOLLTE die in der Institution vorhandenen Vorgaben zum Umgang mit Identitäten und Berechtigungen abbilden können. Das ausgewählte Identitäts- und Berechtigungsmanagement-System SOLLTE den Grundsatz der Funktionstrennung unterstützen. Das Identitäts- und Berechtigungsmanagement-System SOLLTE angemessen vor Angriffen geschützt werden.

ORP.4.A18 Einsatz eines zentralen Authentisierungsdienstes (S) [IT-Betrieb]

Um ein zentrales Identitäts- und Berechtigungsmanagement aufzubauen, SOLLTE ein zentraler netzbasierter Authentisierungsdienst eingesetzt werden. Der Einsatz eines zentralen netzbasierten Authentisierungsdienstes SOLLTE sorgfältig geplant werden. Dazu SOLLTEN die Sicherheitsanforderungen dokumentiert werden, die für die Auswahl eines solchen Dienstes relevant sind.

ORP.4.A19 Einweisung aller Mitarbeitenden in den Umgang mit Authentisierungsverfahren und -mechanismen (S) [Benutzende, IT-Betrieb]

Alle Mitarbeitende SOLLTEN in den korrekten Umgang mit dem Authentisierungsverfahren eingewiesen werden. Es SOLLTE verständliche Richtlinien für den Umgang mit Authentisierungsverfahren geben. Die Mitarbeitenden SOLLTEN über relevante Regelungen informiert werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

ORP.4.A20 Notfallvorsorge für das Identitäts- und Berechtigungsmanagement-System (H) [IT-Betrieb]

Es SOLLTE geprüft werden, inwieweit ein ausgefallenes Identitäts- und Berechtigungsmanagement-System sicherheitskritisch für die Geschäftsprozesse ist. Es SOLLTEN Vorkehrungen getroffen werden, um bei einem ausgefallenen Identitäts- und Berechtigungsmanagement-System weiterhin arbeitsfähig zu sein. Insbesondere SOLLTE das im Notfallkonzept vorgesehene Berechtigungskonzept weiterhin anwendbar sein, wenn das Identitäts- und Berechtigungsmanagement-System ausgefallen ist.

ORP.4.A21 Mehr-Faktor-Authentisierung (H) [IT-Betrieb]

Es SOLLTE eine sichere Mehr-Faktor-Authentisierung, z. B. mit kryptografischen Zertifikaten, Chipkarten oder Token, zur Authentisierung verwendet werden.

ORP.4.A24 Vier-Augen-Prinzip für administrative Tätigkeiten (H) [IT-Betrieb]

Administrative Tätigkeiten SOLLTEN nur durch zwei Personen durchgeführt werden können. Dazu SOLLTEN bei Mehr-Faktor-Authentisierung die Faktoren auf die zwei Personen verteilt werden. Bei der Nutzung von Passwörtern SOLLTEN diese in zwei Teile zerlegt werden und jede der zwei Personen enthält einen Teil.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 „Information technology – Security techniques – Information security management systems – Requirements“ im Anhang A.9 Zugangssteuerung Vorgaben für die Identitäts- und Berechtigungsmanagement.

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 29146:2016 „Information technology – Security techniques – A framework for access management“ Vorgaben für die Identitäts- und Berechtigungsmanagement.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ im Kapitel TS1.4 Identity and Access Management Vorgaben für die Identitäts- und Berechtigungsmanagement.

Das National Institute of Standards and Technology (NIST) gibt in der NIST Special Publication 800-53A, insbesondere Bereiche AC und IA, Hinweise für Identitäts- und Berechtigungsmanagement.



ORP.5 Compliance Management (Anforderungsmanagement)

1. Beschreibung

1.1. Einleitung

In jeder Institution gibt es relevante gesetzliche, vertragliche und sonstige Vorgaben, wie z. B. interne Richtlinien, die beachtet werden müssen. Viele dieser Vorgaben haben direkte oder indirekte Auswirkungen auf das Informationssicherheitsmanagement.

Die Anforderungen unterscheiden sich dabei je nach Branche, Land und anderen Rahmenbedingungen. Darüber hinaus unterliegt beispielsweise eine Behörde anderen externen Regelungen als eine Aktiengesellschaft. Die Leitungsebene der Institution muss die Einhaltung der Anforderungen („Compliance“) durch angemessene Überwachungsmaßnahmen sicherstellen.

Je nach Größe einer Institution kann diese verschiedene Managementprozesse haben, die sich mit unterschiedlichen Aspekten des Risikomanagements beschäftigen. Dazu zählen beispielsweise Informationssicherheitsmanagement, Datenschutzmanagement, Compliance Management und Controlling. Die verschiedenen Einheiten sollten vertrauensvoll zusammenarbeiten, um Synergieeffekte zu nutzen und Konflikte frühzeitig auszuräumen.

1.2. Zielsetzung

Ziel des Bausteins ist es, aufzuzeigen, wie sich Zuständige einen Überblick über die verschiedenen Anforderungen an die einzelnen Bereiche einer Institution verschaffen können. Dazu sind geeignete Sicherheitsanforderungen zu identifizieren und umzusetzen, um Verstöße gegen diese Vorgaben zu vermeiden.

1.3. Abgrenzung und Modellierung

Der Baustein ORP.5 *Compliance Management (Anforderungsmanagement)* ist für den gesamten Informationsverbund einmal anzuwenden.

Die Verpflichtung der Mitarbeitenden zur Einhaltung der in diesem Baustein identifizierten gesetzlichen, vertraglichen und sonstigen Vorgaben ist nicht Bestandteil dieses Bausteins, sondern wird im Baustein ORP.2 *Personal* behandelt.

In diesem Baustein wird nicht auf spezifische Gesetze, vertragliche Regelungen oder sonstige Richtlinien eingegangen.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein ORP.5 *Compliance Management (Anforderungsmanagement)* von besonderer Bedeutung.

2.1. Verstoß gegen rechtliche Vorgaben

Wird Informationssicherheit fehlerhaft oder nur spärlich umgesetzt, können Institutionen gegen gesetzliche Regelungen oder vertragliche Vereinbarungen verstoßen. Institutionen müssen außerdem viele verschiedene branchenspezifische, nationale und internationale rechtliche Rahmenbedingungen beachten. Da dies sehr komplex sein kann, können Anwendende unabsichtlich gegen rechtliche Vorgaben verstoßen oder dies sogar vorsätzlich in Kauf nehmen. So bieten z. B. viele Cloud-Dienstleistende ihre Services in einem internationalen Umfeld an. Damit unter-

liegen die Anbietenden oft anderen nationalen Gesetzgebungen. Häufig sehen Cloud-Anwendende nur auf niedrige Kosten und schätzen die zu beachtenden rechtlichen Rahmenbedingungen, wie Datenschutz, Informationspflichten, Insolvenzrecht, Haftung oder den Informationszugriff durch Dritte, falsch ein.

2.2. Unzulässige Weitergabe von Informationen

Durch falsches Verhalten von Mitarbeitenden kann es dazu kommen, dass schützenswerte Informationen unzulässig weitergegeben werden. So können beispielsweise vertrauliche Informationen in Hörweite fremder Personen diskutiert werden, etwa in Pausengesprächen von Konferenzen oder über Mobiltelefonate in öffentlichen Umgebungen. Ebenso denkbar ist, dass der oder die Vorgesetzte einer Fachabteilung Mitarbeitende verdächtigt, mit der Konkurrenz zusammenzuarbeiten. Um ihm dies nachzuweisen, bittet er oder sie den IT-Betrieb, „auf dem kleinen Dienstweg“ einen Einblick in die E-Mails dieser Mitarbeitenden zu erhalten. Der IT-Betrieb kommt der Bitte nach, ohne die hierfür notwendigen Zustimmungen einzuholen.

2.3. Unzureichende Identifikationsprüfung von Kommunikationspartnern und -partnerinnen

In persönlichen Gesprächen, am Telefon oder auch in E-Mails sind viele Mitarbeitende bereit, weit mehr Informationen preiszugeben, als sie das in z. B. in einem Brief oder in größerer Runde tun würden. Darüber hinaus wird die Identität der Kommunikationspartner und -partnerinnen in der Regel nicht hinterfragt, da dies als unhöflich empfunden wird. Ebenso werden häufig Berechtigungen nicht ausreichend geprüft, sondern aus der (behaupteten) Rolle implizit abgeleitet. So können Mitarbeitende eine E-Mail von angeblichen Bekannten ihrer Vorgesetzten erhalten, mit der vermeintlich die schnelle Überweisung eines ausstehenden Betrages vereinbart wurde. Oder eine fremde Person in Arbeitskleidung mit Montagekoffer erhält Zutritt zum Rechenzentrum, nachdem er etwas von „Wasserrohren“ erwähnt.

2.4. Unbeabsichtigte Weitergabe interner Informationen

Bei der Weitergabe von Informationen kommt es immer wieder vor, dass neben den gewünschten Inhalten versehentlich auch andere Angaben übermittelt werden. Dadurch können vertrauliche Informationen in die falschen Hände geraten. Dabei kann es sich z. B. um alte Dateien oder Restinformationen auf weitergegebenen Datenträgern handeln. Auch könnten Benutzende falsche Daten übermitteln oder sie an falsche Empfänger versenden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins ORP.5 *Compliance Management (Anforderungsmanagement)* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Compliance-Beauftragte
Weitere Zuständigkeiten	Zentrale Verwaltung, Vorgesetzte, Institutionsleitung

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

ORP.5.A1 Identifikation der Rahmenbedingungen (B) [Zentrale Verwaltung, Institutionsleitung]

Alle gesetzlichen, vertraglichen und sonstigen Vorgaben mit Auswirkungen auf das Informationssicherheitsmanagement MÜSSEN identifiziert und dokumentiert werden. Die für die einzelnen Bereiche der Institution relevanten gesetzlichen, vertraglichen und sonstigen Vorgaben SOLLTEN in einer strukturierten Übersicht herausgearbeitet werden. Die Dokumentation MUSS auf dem aktuellen Stand gehalten werden.

ORP.5.A2 Beachtung der Rahmenbedingungen (B) [Vorgesetzte, Zentrale Verwaltung, Institutionsleitung]

Die als sicherheitsrelevant identifizierten Anforderungen MÜSSEN bei der Planung und Konzeption von Geschäftsprozessen, Anwendungen und IT-Systemen oder bei der Beschaffung neuer Komponenten einfließen.

Führungskräfte, die eine rechtliche Verantwortung für die Institution tragen, MÜSSEN für die Einhaltung der gesetzlichen, vertraglichen und sonstigen Vorgaben sorgen. Die Verantwortlichkeiten und Zuständigkeiten für die Einhaltung dieser Vorgaben MÜSSEN festgelegt sein.

Es MÜSSEN geeignete Maßnahmen identifiziert und umgesetzt werden, um Verstöße gegen relevante Anforderungen zu vermeiden. Wenn solche Verstöße erkannt werden, MÜSSEN sachgerechte Korrekturmaßnahmen ergriffen werden, um die Abweichungen zu beheben.

ORP.5.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

ORP.5.A4 Konzeption und Organisation des Compliance Managements (S) [Institutionsleitung]

In der Institution SOLLTE ein Prozess aufgebaut werden, um alle relevanten gesetzlichen, vertraglichen und sonstigen Vorgaben mit Auswirkungen auf das Informationssicherheitsmanagement zu identifizieren. Es SOLLTEN geeignete Prozesse und Organisationsstrukturen aufgebaut werden, um basierend auf der Identifikation und Beachtung der rechtlichen Rahmenbedingungen, den Überblick über die verschiedenen rechtlichen Anforderungen an die einzelnen Bereiche der Institution zu gewährleisten. Dafür SOLLTEN Zuständige für das Compliance Management festgelegt werden.

Compliance-Beauftragte und Informationssicherheitsbeauftragte SOLLTEN sich regelmäßig austauschen. Sie SOLLTEN gemeinsam Sicherheitsanforderungen ins Compliance Management integrieren, sicherheitsrelevante Anforderungen in Sicherheitsmaßnahmen überführen und deren Umsetzung kontrollieren.

ORP.5.A5 Ausnahmegenehmigungen (S) [Vorgesetzte]

Ist es in Einzelfällen erforderlich, von getroffenen Regelungen abzuweichen, SOLLTE die Ausnahme begründet und durch eine autorisierte Stelle nach einer Risikoabschätzung genehmigt werden. Es SOLLTE ein Genehmigungsverfahren für Ausnahmegenehmigungen geben. Es SOLLTE eine Übersicht über alle erteilten Ausnahmegenehmigungen erstellt und gepflegt werden. Ein entsprechendes Verfahren für die Dokumentation und ein Überprüfungsprozess SOLLTE etabliert werden. Alle Ausnahmegenehmigungen SOLLTEN befristet sein.

ORP.5.A6 ENTFALLEN (S)

Diese Anforderung ist entfallen.

ORP.5.A7 ENTFALLEN (S)

Diese Anforderung ist entfallen.

ORP.5.A8 Regelmäßige Überprüfungen des Compliance Managements (S)

Es SOLLTE ein Verfahren etabliert sein, wie das Compliance Management und die sich daraus ergebenden Anforderungen und Maßnahmen regelmäßig auf ihre Effizienz und Effektivität überprüft werden (siehe auch DER.3.1 *Audits und Revisionen*). Es SOLLTE regelmäßig geprüft werden, ob die Organisationsstruktur und die Prozesse des Compliance Managements angemessen sind.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

ORP.5.A9 ENTFALLEN (H)

Diese Anforderung ist entfallen.

ORP.5.A10 ENTFALLEN (H)

Diese Anforderung ist entfallen.

ORP.5.A11 ENTFALLEN (H)

Diese Anforderung ist entfallen.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO 19600:2014 „Compliance management systems – Guidelines“ Richtlinien für ein Compliance Management System.

Ebenso geht die ISO in der Norm ISO/IEC 27001:2013 „Information technology – Security technique – Code of practice for information security controls“ im Kapitel 18 auf Anforderungsmanagement ein.

Das Institut der Wirtschaftsprüfer (IDW) definiert in der IDW Verlautbarung IDW PS 980 „Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen“ Anhaltspunkte für die Prüfung von Compliance Management Systemen.

CON: Konzepte und Vorgehensweisen



CON.1 Kryptokonzept

1. Beschreibung

1.1. Einleitung

Kryptografie ist ein weit verbreitetes Mittel, um Informationssicherheit in den Schutzziele Vertraulichkeit, Integrität und Authentizität zu gewährleisten. Damit ist es beispielsweise möglich, Informationen so zu verschlüsseln, dass deren Inhalt ohne den zugehörigen Schlüssel nicht lesbar ist. Bei symmetrischen Verfahren wird derselbe Schlüssel zum Ver- und Entschlüsseln verwendet, bei asymmetrischen Verfahren ein Schlüssel zum Verschlüsseln und ein anderer zum Entschlüsseln.

In den unterschiedlichsten IT-Umgebungen, wie beispielsweise Client-Server-Umgebungen, können lokal gespeicherte Informationen und auch die zu übertragenden Informationen zwischen Kommunikationspartnern und -partnerinnen wirkungsvoll durch kryptografische Verfahren geschützt werden. Kryptografische Verfahren können dabei in Hard- oder Software-Komponenten implementiert sein (im Folgenden als Hard- oder Software mit kryptografischen Funktionen zusammengefasst).

Der alleinige technische Einsatz von kryptografischen Verfahren genügt nicht, um die Vertraulichkeit, Integrität und Authentizität der Informationen zu gewährleisten. Darüber hinaus werden organisatorische Maßnahmen benötigt. Um Informationen effektiv zu schützen, ist es erforderlich, das Thema Kryptografie ganzheitlich im Rahmen eines Kryptokonzepts zu behandeln.

1.2. Zielsetzung

Dieser Baustein beschreibt, wie ein Kryptokonzept erstellt werden sollte und wie damit Informationen in Institutionen kryptografisch abgesichert werden können.

1.3. Abgrenzung und Modellierung

Der Baustein CON.1 *Kryptokonzept* ist einmal auf den Informationsverbund anzuwenden. In diesem Baustein werden organisatorische und technische Anforderungen für Hard- oder Software mit kryptografischen Funktionen sowie kryptografische Verfahren behandelt. Die mit dem Betrieb von Hard- oder Software mit kryptografischen Funktionen zusammenhängenden Kern-IT-Aufgaben werden nicht thematisiert. Dafür müssen die Anforderungen der Bausteine aus der Schicht OPS.1.1 *Kern-IT-Betrieb* erfüllt werden.

Wie Anwendungen (z. B. Ende-zu-Ende-Verschlüsselung bei E-Mails), einzelne IT-Systeme (z. B. Laptops) oder Kommunikationsverbindungen kryptografisch abgesichert werden können, ist ebenfalls nicht Gegenstand dieses Bausteins. Diese Themen werden in den entsprechenden Bausteinen der Schichten APP *Anwendungen*, SYS *IT-Systeme* und NET *Netze und Kommunikation* behandelt.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein CON.1 *Kryptokonzept* von besonderer Bedeutung.

2.1. Unzureichendes Schlüsselmanagement bei Verschlüsselung

Durch ein unzureichendes Schlüsselmanagement könnten bei Angriffen unverschlüsselte Informationen offengelegt werden. So kann es beispielsweise sein, dass sich aufgrund fehlender Regelungen verschlüsselte Informationen

mit den dazugehörigen Schlüsseln auf demselben Datenträger befinden oder über denselben Kommunikationskanal unverschlüsselt übertragen werden. In diesen Fällen kann bei symmetrischen Verfahren jede Person, die auf den Datenträger oder den Kommunikationskanal zugreifen kann, die Informationen entschlüsseln.

Ein unzureichendes oder fehlendes Schlüsselmanagement kann auch die Verfügbarkeit von Anwendungen bedrohen, wenn zum Beispiel kryptographische Funktionen nicht mehr benutzbar sind, nachdem die Gültigkeitsdauer von Schlüsseln oder Zertifikaten abgelaufen ist.

2.2. Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von Hard- oder Software mit kryptografischen Funktionen

Wenn Institutionen Hard- oder Software mit kryptografischen Funktionen einsetzen, müssen sie diverse gesetzliche Rahmenbedingungen beachten. In einigen Ländern dürfen beispielsweise kryptografische Verfahren nur mit staatlicher Genehmigung eingesetzt werden, sodass der Einsatz von Hard- oder Software mit starken kryptografischen Funktionen erheblich eingeschränkt ist. Das kann dazu führen, dass Empfänger oder Empfängerinnen in solchen Ländern verschlüsselte Datensätze nicht lesen können, da sie die benötigte Hard- oder Software mit kryptografischen Funktionen nicht einsetzen dürfen. Im ungünstigsten Fall würden Empfänger oder Empfängerinnen sich sogar strafbar machen, wenn sie die benötigte Hard- oder Software mit kryptografischen Funktionen ungenehmigt einsetzen würden. Oder diese Situation verleitet die an der Kommunikation beteiligten Personen dazu, die Informationen unverschlüsselt auszutauschen, was wiederum zu einer Vielzahl von Gefährdungen der Vertraulichkeit, Integrität und Authentizität der ausgetauschten Informationen führen kann.

Es kann sogar die Situation auftreten, dass die rechtlichen Bestimmungen eines Landes festlegen, dass angemessene Kryptografie einzusetzen ist, während die Bestimmungen eines anderen Landes dies genau verbieten oder eine staatliche Möglichkeit zur Entschlüsselung vorsehen. So können beispielsweise europäische Datenschutzbestimmungen vorschreiben, dass angemessene kryptografische Verfahren eingesetzt werden müssen, um personenbezogene Daten zu schützen. Soll nun aus einem entsprechenden europäischen Land in ein anderes Land kommuniziert werden, in dem der Einsatz von Kryptografie stark reglementiert ist und in dem konkreten Fall nicht genehmigt ist, dann ist eine legale Kommunikation zwischen zwei Personen aus den jeweiligen Ländern nicht möglich.

2.3. Vertraulichkeits- oder Integritätsverlust von Informationen durch Fehlverhalten

Werden kryptographische Funktionen nicht oder nicht richtig verwendet, so können sie den damit beabsichtigten Schutz von Informationen nicht gewährleisten. Setzt eine Institution beispielsweise Hard- oder Software mit kryptografischen Funktionen ein, die sehr kompliziert zu bedienen ist, könnten die Benutzenden auf Verschlüsselung der Information verzichten und sie stattdessen im Klartext übertragen. Dadurch können die übertragenen Informationen bei einem Angriff mitgelesen werden.

Wird Hard- oder Software mit kryptografischen Funktionen falsch bedient, kann dies auch dazu führen, dass vertrauliche Informationen bei Angriffen abgegriffen werden, etwa, wenn diese im Klartext übertragen werden, weil versehentlich der Klartext-Modus aktiviert wurde.

2.4. Schwachstellen oder Fehler in Hard- oder Software mit kryptografischen Funktionen

Schwachstellen oder Fehler in Hard- oder Software mit kryptografischen Funktionen beeinträchtigen die Sicherheit der eingesetzten kryptografischen Verfahren. Sie können etwa dazu führen, dass die damit geschützten Informationen mitgelesen werden.

So setzt eine Vielzahl von kryptografischen Verfahren auf Zufallsgeneratoren, um sichere Schlüssel z. B. für eine Kommunikationsverbindung zu generieren. Auch wenn ein solches Verfahren als prinzipiell und konzeptionell sicher gilt, kann ein Fehler in der Hard- oder Software-Implementierung dazu führen, dass z. B. vorhersagbare Zufallszahlen generiert werden und somit auch die damit verbundenen kryptografischen Schlüssel rekonstruiert werden können. Dadurch können verschlüsselte Informationen ausgespäht werden, was wiederum weitreichende Folgen nach sich ziehen kann.

2.5. Ausfall von Hardware mit kryptografischen Funktionen

Hardware mit kryptografischen Funktionen (z. B. Chipkarten zur Laufwerksverschlüsselung) kann durch technische Defekte, Stromausfälle oder absichtliche Zerstörung ausfallen. Dadurch könnten bereits verschlüsselte Informationen nicht mehr entschlüsselt werden, solange die erforderliche Hardware nicht verfügbar ist. Als Folge können ganze Prozessketten stillstehen, z. B. wenn weitere Anwendungen auf die Informationen angewiesen sind.

2.6. Unsichere kryptografische Algorithmen

Unsichere oder veraltete kryptografische Algorithmen lassen sich bei einem Angriff mit geringem Aufwand brechen. Bei Verschlüsselungsalgorithmen bedeutet dies, dass es gelingt, aus dem verschlüsselten Text den ursprünglichen Klartext zu ermitteln, ohne dass bei dem Angriff zusätzliche Informationen zur Verfügung stehen, wie z. B. den verwendeten kryptografischen Schlüssel. Werden unsichere kryptografische Algorithmen eingesetzt, können Angreifende den kryptografischen Schutz unterlaufen und somit auf schützenswerte Informationen der Institution zugreifen. Selbst wenn in einer Institution ausschließlich sichere (z. B. zertifizierte) Hard- oder Software mit kryptografischen Funktionen eingesetzt wird, kann die Kommunikation trotzdem unsicher werden. Das ist beispielsweise der Fall, wenn der Kommunikationspartner oder die Kommunikationspartnerin kryptografische Verfahren einsetzt, die nicht dem Stand der Technik entsprechen.

2.7. Fehler in verschlüsselten Informationen oder kryptografischen Schlüsseln

Werden Informationen verschlüsselt und die Chiffre im Anschluss verändert, lassen sich die verschlüsselten Informationen eventuell nicht mehr korrekt entschlüsseln. Je nach Betriebsart der Verschlüsselungsroutinen kann dies bedeuten, dass nur wenige Bytes oder sämtliche Informationen verloren sind. Ist keine Datensicherung vorhanden, sind solche Informationen verloren. Dieser Umstand kann auch bei Angriffen ausgenutzt werden, indem nur ein minimaler Anteil der Chiffre verändert wird und dadurch die verschlüsselten Informationen vollständig verloren gehen.

Noch kritischer kann sich ein Fehler in den verwendeten kryptografischen Schlüsseln auswirken. Schon die Änderung eines einzigen Bits eines kryptografischen Schlüssels führt dazu, dass sämtliche damit verschlüsselten Informationen nicht mehr entschlüsselt werden können.

2.8. Kompromittierung kryptografischer Schlüssel

Die Sicherheit kryptografischer Verfahren hängt entscheidend davon ab, wie vertraulich die verwendeten kryptografischen Schlüssel bleiben. Daher wird bei einem Angriff in der Regel versucht, die verwendeten Schlüssel zu erlangen oder zu ermitteln. Das könnte z. B. gelingen, indem flüchtige Speicher ausgelesen oder ungeschützte Schlüssel gefunden werden, die beispielsweise in einer Datensicherung oder einer Konfigurationsdatei hinterlegt sind. Sind die verwendeten Schlüssel und das eingesetzte Kryptoverfahren bekannt, dann können die Informationen relativ leicht entschlüsselt werden.

2.9. Gefälschte Zertifikate

Zertifikate dienen dazu, einen öffentlichen kryptografischen Schlüssel an eine Person, ein IT-System oder eine Institution zu binden. Diese Bindung des Schlüssels wird wiederum kryptografisch mittels einer digitalen Signatur häufig von einer vertrauenswürdigen dritten Stelle abgesichert.

Die Zertifikate werden von Dritten benutzt, um digitale Signaturen der im Zertifikat ausgewiesenen Person, des IT-Systems oder der Institution zu prüfen. Alternativ kann der im Zertifikat hinterlegte Schlüssel für ein asymmetrisches Verschlüsselungsverfahren benutzt werden, um die Informationen für den Zertifikatsinhaber oder die Zertifikatsinhaberin zu verschlüsseln.

Ist ein solches Zertifikat gefälscht, dann werden digitale Signaturen fälschlicherweise als korrekt geprüft und der Person, dem IT-System oder der Institution im Zertifikat zugeordnet. Oder es werden Informationen mit einem möglicherweise unsicheren Schlüssel verschlüsselt und versandt.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins CON.1 *Kryptokonzept* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Informationssicherheitsbeauftragte (ISB)
Weitere Zuständigkeiten	Fachverantwortliche, IT-Betrieb, Benutzende

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

CON.1.A1 Auswahl geeigneter kryptografischer Verfahren (B) [Fachverantwortliche]

Es MÜSSEN geeignete kryptografische Verfahren ausgewählt werden. Dabei MUSS sichergestellt sein, dass etablierte Algorithmen verwendet werden, die von der Fachwelt intensiv untersucht wurden und von denen keine Sicherheitslücken bekannt sind. Ebenso MÜSSEN aktuell empfohlene Schlüssellängen verwendet werden. Um eine geeignete Schlüssellänge auszuwählen, SOLLTE berücksichtigt werden, wie lange das kryptografische Verfahren eingesetzt werden soll. Bei einer längeren Einsatzdauer SOLLTEN entsprechend längere Schlüssellängen eingesetzt werden.

CON.1.A2 Datensicherung beim Einsatz kryptografischer Verfahren (B) [IT-Betrieb]

In Datensicherungen MÜSSEN kryptografische Schlüssel vom IT-Betrieb derart gespeichert oder aufbewahrt werden, dass Unbefugte nicht darauf zugreifen können. Langlebige kryptografische Schlüssel MÜSSEN offline, außerhalb der eingesetzten IT-Systeme, aufbewahrt werden.

Bei einer Langzeitspeicherung verschlüsselter Informationen SOLLTE regelmäßig geprüft werden, ob die verwendeten kryptografischen Algorithmen und die Schlüssellängen noch für die jeweiligen Informationen geeignet sind. Der IT-Betrieb MUSS sicherstellen, dass auf verschlüsselt gespeicherte Informationen auch nach längeren Zeiträumen noch zugegriffen werden kann. Verwendete Hard- oder Software mit kryptografischen Funktionen SOLLTE archiviert werden.

CON.1.A4 Geeignetes Schlüsselmanagement (B)

In einem geeigneten Schlüsselmanagement für kryptografische Hard oder Software MUSS festgelegt werden, wie Schlüssel und Zertifikate erzeugt, gespeichert, ausgetauscht und wieder gelöscht oder vernichtet werden. Es MUSS ferner festgelegt werden, wie die Integrität und Authentizität der Schlüssel sichergestellt wird.

Kryptografische Schlüssel SOLLTEN immer mit geeigneten Schlüsselgeneratoren und in einer sicheren Umgebung erzeugt werden. In Hard- oder Software mit kryptografischen Funktionen SOLLTEN voreingestellte Schlüssel (ausgenommen öffentliche Zertifikate) ersetzt werden. Ein Schlüssel SOLLTE möglichst nur einem Einsatzzweck dienen. Insbesondere SOLLTEN für die Verschlüsselung und Signaturbildung unterschiedliche Schlüssel benutzt werden. Kryptografische Schlüssel SOLLTEN mit sicher geltenden Verfahren ausgetauscht werden.

Wenn öffentliche Schlüssel von Dritten verwendet werden, MUSS sichergestellt sein, dass die Schlüssel authentisch sind und die Integrität der Schlüsseldaten gewährleistet ist.

Geheime Schlüssel MÜSSEN sicher gespeichert und vor unbefugtem Zugriff geschützt werden. Alle kryptografischen Schlüssel SOLLTEN hinreichend häufig gewechselt werden. Grundsätzlich SOLLTE geregelt werden, wie mit abgelaufenen Schlüsseln und damit verbundenen Signaturen verfahren wird. Falls die Gültigkeit von Schlüsseln oder Zertifikaten zeitlich eingeschränkt wird, dann MUSS durch die Institution sichergestellt werden, dass die zeitlich eingeschränkten Zertifikate oder Schlüssel rechtzeitig erneuert werden.

Eine Vorgehensweise SOLLTE für den Fall festgelegt werden, dass ein privater Schlüssel offengelegt wird. Alle erzeugten kryptografischen Schlüssel SOLLTEN sicher aufbewahrt und verwaltet werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

CON.1.A3 ENTFALLEN (S)

Diese Anforderung ist entfallen.

CON.1.A5 Sicheres Löschen und Vernichten von kryptografischen Schlüsseln (S) [IT-Betrieb, Benutzende]

Nicht mehr benötigte private Schlüssel SOLLTEN sicher gelöscht oder vernichtet werden. Die Vorgehensweisen und eingesetzten Methoden, um nicht mehr benötigte private Schlüssel zu löschen oder zu vernichten, SOLLTEN im Kryptokonzept dokumentiert werden.

CON.1.A6 ENTFALLEN (S)

Diese Anforderung ist entfallen.

CON.1.A7 ENTFALLEN (S)

Diese Anforderung ist entfallen.

CON.1.A8 ENTFALLEN (S)

Diese Anforderung ist entfallen.

CON.1.A9 Festlegung von Kriterien für die Auswahl von Hard- oder Software mit kryptografischen Funktionen (S) [Fachverantwortliche]

Im Kryptokonzept SOLLTE festgelegt werden, anhand welcher Kriterien und Anforderungen Hard- oder Software mit kryptografischen Funktionen ausgesucht wird. Hierbei SOLLTEN Aspekte wie

- Funktionsumfang,
- Interoperabilität,
- Wirtschaftlichkeit,
- Fehlbedienungs- und Fehlfunktionssicherheit,
- technische Aspekte,
- personelle und organisatorische Aspekte,
- Lebensdauer von kryptografischen Verfahren und der eingesetzten Schlüssellängen sowie
- gesetzliche Rahmenbedingungen
- internationale rechtliche Aspekte wie Export- und Importbeschränkungen für Hard- oder Software mit kryptografischen Funktionen, wenn die kryptografischen Verfahren auch im Ausland eingesetzt werden
- Datenschutz

berücksichtigt und im Kryptokonzept dokumentiert werden. Dabei SOLLTE grundsätzlich zertifizierte Hard- oder Software mit kryptografischen Funktionen, deren Zertifizierung die jeweils relevanten Aspekte der Kryptografie umfasst, bevorzugt ausgewählt werden.

CON.1.A10 Erstellung eines Kryptokonzepts (S)

Ausgehend von dem allgemeinen Sicherheitskonzept der Institution SOLLTE ein Kryptokonzept für Hard- oder Software mit kryptografischen Funktionen erstellt werden. Im Kryptokonzept SOLLTE beschrieben werden,

- wie die Datensicherungen von kryptografischen Schlüsseln durchgeführt werden,
- wie das Schlüsselmanagement von kryptografischen Schlüsseln ausgestaltet ist sowie
- wie das Krypto-Kastaster erhoben wird.

Weiterhin SOLLTE im Kryptokonzept beschrieben werden, wie sichergestellt wird, dass kryptografische Funktionen von Hard- oder Software sicher konfiguriert und korrekt eingesetzt werden. Im Kryptokonzept SOLLTEN alle technischen Vorgaben für Hard- und Software mit kryptografischen Funktionen beschrieben werden (z. B. Anforderungen, Konfiguration oder Parameter). Um geeignete kryptografische Verfahren auszuwählen, SOLLTE die BSI TR 02102 berücksichtigt werden.

Wird das Kryptokonzept verändert oder von ihm abgewichen, SOLLTE dies mit dem oder der ISB abgestimmt und dokumentiert werden. Das Kryptokonzept SOLLTE allen bekannt sein, die kryptografische Verfahren einsetzen. Außerdem SOLLTE es bindend für ihre Arbeit sein. Insbesondere der IT-Betrieb SOLLTE die kryptografischen Vorgaben des Kryptokonzepts umsetzen.

CON.1.A15 Reaktion auf praktische Schwächung eines Kryptoverfahrens (S)

Die Institution SOLLTE mindestens jährlich anhand des Krypto-Katasters überprüfen, ob die eingesetzten kryptografischen Verfahren und die zugehörigen Parameter noch ausreichend sicher sind und keine bekannten Schwachstellen aufweisen.

Im Kryptokonzept SOLLTE ein Prozess für den Fall definiert und dokumentiert werden, dass Schwachstellen in kryptografischen Verfahren auftreten. Dabei SOLLTE sichergestellt werden, dass das geschwächte kryptografische Verfahren entweder abgesichert oder durch eine geeignete Alternative abgelöst wird, sodass hieraus kein Sicherheitsrisiko entsteht.

CON.1.A19 Erstellung eines Krypto-Katasters (S) [IT-Betrieb]

Für jede Gruppe von IT-Systemen SOLLTEN folgende Informationen im Krypto-Kataster festgehalten werden:

- Einsatzzweck (z. B. Festplattenverschlüsselung oder Verschlüsselung einer Kommunikationsverbindung)
- Zuständige
- eingesetztes kryptografische Verfahren
- eingesetzte Hard- oder Software mit kryptografischen Funktionen
- eingesetzte sicherheitsrelevante Parameter (z. B. Schlüssellängen)

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse

CON.1.A11 Test von Hardware mit kryptografischen Funktionen (H) [IT-Betrieb]

Im Kryptokonzept SOLLTEN Testverfahren für Hardware mit kryptografischen Funktionen festgelegt werden. Bevor Hardware mit kryptografischen Funktionen eingesetzt wird, sollte getestet werden, ob die kryptografischen Funktionen korrekt funktionieren.

Wenn ein IT-System geändert wird, SOLLTE getestet werden, ob die eingesetzte kryptografische Hardware noch ordnungsgemäß funktioniert. Die Konfiguration der kryptografischen Hardware SOLLTE regelmäßig überprüft werden.

CON.1.A12 ENTFALLEN (H)

Diese Anforderung ist entfallen.

CON.1.A13 ENTFALLEN (H)

Diese Anforderung ist entfallen.

CON.1.A14 ENTFALLEN (H)

Diese Anforderung ist entfallen.

CON.1.A16 Physische Absicherung von Hardware mit kryptografischen Funktionen (H) [IT-Betrieb]

Im Kryptokonzept SOLLTE festgelegt werden, wie der IT-Betrieb sicherstellt, dass nicht unautorisiert physisch auf Hardware mit kryptografischen Funktionen zugegriffen werden kann.

CON.1.A17 Abstrahlsicherheit (H) [IT-Betrieb]

Es SOLLTE geprüft werden, ob zusätzliche Maßnahmen hinsichtlich der Abstrahlsicherheit notwendig sind. Dies SOLLTE insbesondere dann geschehen, wenn staatliche Verschlusssachen (VS) der Geheimhaltungsgrade VS-VERTRAULICH und höher verarbeitet werden. Betroffene Maßnahmen hinsichtlich der Abstrahlsicherheit SOLLTEN im Kryptokonzept dokumentiert werden.

CON.1.A18 Kryptografische Ersatzhardware (H) [IT-Betrieb]

Hardware mit kryptografischen Funktionen (z. B. Hardware-Token für Zwei-Faktor-Authentifizierung) SOLLTE vorrätig sein. Im Kryptokonzept SOLLTE dokumentiert werden, für welche Hardware mit kryptografischen Funktionen Ersatzhardware zur Verfügung steht und wie diese ausgetauscht werden kann.

CON.1.A20 Manipulationserkennung für Hard- oder Software mit kryptografischen Funktionen (H)

Hard- und Software mit kryptografischen Funktionen SOLLTE auf Manipulationsversuche hin überwacht werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) behandelt das Thema Kryptografie in der Norm ISO/IEC 27001:2013 im Annex A.10 anhand von zwei Richtlinien.

Für die Auswahl von Verschlüsselungsverfahren und Schlüssellängen sollte die technische Richtlinie „BSI-TR-02102: Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ des BSI beachtet werden.

Das Information Security Forum (ISF) hat in seinem Standard „The Standard of Good Practice for Information Security“ in der „Area TS2 Cryptography“ Anforderungen an Kryptokonzepte erarbeitet.



CON.2 Datenschutz

1. Beschreibung

1.1. Einleitung

Im Gegensatz zur Informationssicherheit, die primär dem Schutz der datenverarbeitenden Institution dient, ist es Aufgabe des Datenschutzes, natürliche Personen davor zu schützen, dass Institutionen oder Stellen mit ihren Verarbeitungstätigkeiten zu intensiv in die Grundrechte und Grundfreiheiten der Personen eingreifen. Das Grundgesetz für die Bundesrepublik Deutschland gewährleistet das Recht von Bürgerinnen und Bürgern, grundsätzlich selbst über die Verwendung ihrer personenbezogenen Daten zu bestimmen. Die Datenschutzgesetze des Bundes und der Bundesländer nehmen darauf Bezug, wenn sie den Schutz des Rechts auf informationelle Selbstbestimmung hervorheben. Die EU-Grundrechtecharta formuliert in Artikel 8 unmittelbar das Recht auf den Schutz personenbezogener Daten (Absatz 1), hebt die Notwendigkeit einer Rechtsgrundlage zur Datenverarbeitung hervor (Absatz 2) und schreibt die Überwachung der Einhaltung von Datenschutzvorschriften durch eine unabhängige Stelle vor (Absatz 3). Die Datenschutz-Grundverordnung (DSGVO) führt diese Anforderungen der Grundrechtecharta näher aus. Von zentraler Bedeutung ist dabei der Artikel 5 DSGVO, der die Grundsätze für die Verarbeitung personenbezogener Daten auflistet, die teilweise auch als Schutzziele verstanden werden können. Neben der DSGVO sind das Bundesdatenschutzgesetz (BDSG) und die Datenschutzgesetze der Bundesländer sowie weitere bereichsspezifische Regelungen wie beispielsweise das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) zu berücksichtigen.

Zugespißt sind im Rahmen des operativen Datenschutzes vier Typen von Risiken, die mit unterschiedlichen Ausprägungen von Schutzmaßnahmen zu verringern sind, zu unterscheiden:

- Risikotyp A: Der Grundrechtseingriff bei natürlichen Personen durch die Verarbeitung ist nicht hinreichend milde gestaltet.
- Risikotyp B: Die Maßnahmen zur Verringerung der Eingriffsintensität einer Verarbeitung sind, in Bezug auf die Gewährleistungsziele, nicht vollständig oder werden nicht hinreichend wirksam betrieben oder nicht in einem ausreichenden Maße stetig kontrolliert, geprüft und beurteilt.
- Risikotyp C: Die Maßnahmen, die nach der Informationssicherheit geboten sind (vgl. z. B. IT-Grundschutz nach BSI), sind nicht vollständig oder werden nicht hinreichend wirksam betrieben oder werden nicht in einem ausreichenden Maße stetig kontrolliert, geprüft und beurteilt.
- Risikotyp D: Die Maßnahme der Informationssicherheit werden nicht ausreichend datenschutzgerecht, im Sinne des Risikotyp A und Risikotyp B, betrieben.

Die Prüfung der Verhältnismäßigkeit des Grundrechtseingriffs einer Verarbeitung ist nicht vom SDM umfasst. Diese rechtliche Prüfung sowie die Prüfung der Rechtsgrundlage (vergleiche insbesondere Art. 6 und 9 DS-GVO) und des Verarbeitungszwecks müssen vor der Anwendung des SDM erfolgen. Somit ist die Behandlung des zuvor genannten Risikotyps A nicht unmittelbar Gegenstand der Anwendung des SDM. Wird ein oder werden mehrere Risikotypen nicht betrachtet oder nicht hinreichend zwischen den Risiko-Typen differenziert, dann besteht die Gefahr, dass das informationelle Selbstbestimmungsrecht der betroffenen Person nicht gesetzeskonform gewährleistet werden kann.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (kurz: Datenschutzkonferenz, DSK) hat mit dem Standard-Datenschutzmodell (SDM) eine Methode entwickelt, welche die in den deutschen und europäischen Rechtsvorschriften genannten technischen und organisatorischen Maßnahmen auf der Basis von sieben Schutz- beziehungsweise Gewährleistungszielen systematisiert. Damit dient das Modell den für die Datenverarbeitung verantwortlichen und als Auftragsverarbeiter beteiligten Stellen, erforderliche Maßnahmen systematisch zu planen sowie umzusetzen. Es fördert somit die datenschutzgerechte Ausgestaltung und Organisation von informationstechnischen Verfahren, Anwendungen und Infrastrukturen. Andererseits bietet das Mo-

dell den Datenschutzaufsichtsbehörden eine Möglichkeit, mit einer einheitlichen Systematik zu einem transparenten, nachvollziehbaren und belastbaren Gesamturteil über eine Verarbeitung zu gelangen. Das SDM ist als Methode geeignet, die Wirksamkeit der technischen und organisatorischen Maßnahmen einer Datenverarbeitung auf der Grundlage und nach den Kriterien der DSGVO regelmäßig zu überprüfen und fachgerecht zu bewerten.

Das SDM nimmt bei der Auswahl geeigneter technischer und organisatorischer Maßnahmen die Perspektive der Betroffenen und deren Grundrechtsausübung ein und unterscheidet sich daher grundlegend von der Sicht des IT-Grundschutzes. Dieser legt den Schwerpunkt vorrangig auf die Informationssicherheit und soll die datenverarbeitenden Institutionen schützen. Für die Risikobeurteilung und die anschließende Auswahl von Maßnahmen nach dem SDM ist hingegen die Beeinträchtigung maßgeblich, die Betroffene durch die Datenverarbeitung der Institution hinnehmen müssen.

Vor diesem Hintergrund ist zwischen der Auswahl von Maßnahmen zur Gewährleistung der Informationssicherheit für Institutionen und der Auswahl von Maßnahmen zur Gewährleistung des Datenschutzes zu unterscheiden: Die IT-Grundschutz-Methodik dient vorrangig der Informationssicherheit, das Standard-Datenschutzmodell dient der Umsetzung der datenschutzrechtlichen Anforderungen (insbesondere der Grundsätze aus Artikel 5 DSGVO und der Betroffenenrechte aus Kapitel III DSGVO). Das SDM hat daher die folgenden Ansprüche:

- Es überführt datenschutzrechtliche Anforderungen in einen Katalog von Gewährleistungszielen.
- Es gliedert die betrachteten Verfahren in die Komponenten Daten, Systeme und Dienste (inkl. Schnittstellen) sowie Prozesse.
- Es berücksichtigt die Einordnung von Verarbeitungstätigkeiten basierend auf den Risikostufen „kein oder gering“, „normal“ und „hoch“ gemäß DSGVO in die Schutzbedarfsstufen „normal“ und „hoch“, insbesondere mit Auswirkungen auf der Ebene der Sachbearbeitung mit ihren Fachverfahren, die von Anwendungen und IT-Infrastruktur unterstützt werden.
- Es bietet einen Katalog mit standardisierten Schutzmaßnahmen.

Der Referenzmaßnahmen-Katalog des SDM umfasst Maßnahmen, die auf Informationsverbünde oder Verfahren (Verarbeitungen) sowie auf die gesamte Institution im Rahmen eines Datenschutzmanagementprozesses anzuwenden sind.

Die Prüfung der Verhältnismäßigkeit des Grundrechtseingriffs einer Verarbeitung ist nicht vom SDM umfasst. Diese rechtliche Prüfung sowie die Prüfung der Rechtsgrundlage nach Artikel 6 und gegebenenfalls des Artikels 9 DSGVO müssen erfolgen, bevor das SDM angewendet wird. Somit wird der Risikotyp A nicht im Rahmen des SDM selbst behandelt.

1.2. Zielsetzung

Ziel des Bausteins ist es, die Verbindung der Anforderungen des Datenschutzes, die durch das Standard-Datenschutzmodell operationalisiert werden, zum IT-Grundschutz darzustellen.

1.3. Abgrenzung und Modellierung

Der Baustein CON.2 *Datenschutz* ist für den Informationsverbund einmal anzuwenden, wenn personenbezogene Daten unter deutschem oder europäischem Recht verarbeitet werden. Der Baustein CON.2 *Datenschutz* und insbesondere die umfangreichen Erläuterungen in der Einleitung unterstützen somit Anwendende in Deutschland und Europa bei der Orientierung, wenn in der Schutzbedarfsfeststellung Komponenten identifiziert werden, bei denen personenbezogene oder -beziehbare Daten verarbeitet oder sonstig genutzt werden. Dabei sollte dann geprüft werden, ob der Baustein nicht nur auf einzelne Informationsverbünde oder Verfahren, sondern auf die gesamte Institution anzuwenden ist.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein CON.2 *Datenschutz* von besonderer Bedeutung.

2.1. Missachtung von Datenschutzgesetzen oder Nutzung eines unvollständigen Risikomodells

Nach der DSGVO ist die Verarbeitung personenbezogener Daten grundsätzlich verboten. Die Verarbeitung dieser Daten ist nur dann rechtmäßig, wenn die Voraussetzungen des Artikels 6 DSGVO erfüllt sind, also beispielsweise eine Einwilligung der betroffenen Person vorliegt oder eine Rechtsvorschrift die Datenverarbeitung erlaubt. Nicht rechtskonform ist eine Verarbeitung z. B. auch dann, wenn eine Institution eine Datenverarbeitung nicht hinreichend zweckbestimmt, den Zweck überdehnt oder gänzlich zweckungebunden durchführt. Dasselbe gilt, wenn die entsprechende Institution die personenbezogenen Daten intransparent oder ohne integritätssichernde Maßnahmen und ohne Eingriffsmöglichkeiten durch Betroffene verarbeitet.

Aus der Sicht des Datenschutzes ist eine Institution, die personenbezogene Daten verarbeitet (beispielsweise erhebt, speichert, übermittelt oder löscht), grundsätzlich ein Risiko für die davon betroffenen Personen. Dieses Risiko besteht auch dann, wenn die Datenverarbeitung einer Institution rechtskonform ausgestaltet ist.

Ein in der Praxis häufig auftretendes Risiko ist der Zugriff auf Daten, die nicht dem Zweck der ursprünglichen Datenverarbeitung dienen. Dabei kann es sich typischerweise um Zugriffe von ausländischen Konzernmüttern, Sicherheitsbehörden, Banken und Versicherungen, öffentlichen Leistungsverwaltungen, IT-Herstellenden und IT-Dienstleistenden oder Forschungsinstitutionen handeln. Oftmals wird in diesen Kontexten nicht geprüft, ob der Zugriff befugt ist, weil beispielsweise eine langjährig eingefahrene Praxis fortgesetzt wird. Eine andere Möglichkeit ist, dass nachrangige Mitarbeitende das persönliche Risiko scheuen, zu hinterfragen, ob eine hinreichende Rechtsgrundlage vorliegt. Ferner werden aus (teilweise) negativen Prüfergebnissen durch eine Rechtsabteilung oder eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten oft seitens der Verantwortlichen keine Konsequenzen gezogen. Ignorieren Verantwortliche Prüf- oder Beratungsergebnisse, so können sich dadurch Fragen zur Haftung ergeben.

Ein weiteres Risiko sowohl für Personen als auch für verantwortliche Institutionen besteht, wenn für rechtmäßig erfolgte Zugriffe auf IT-Dienste oder die Übermittlung von Datenbeständen durch Dritte keine Standardprozesse vorgesehen sind. Dasselbe gilt, wenn keine Nachweise über die Ordnungsmäßigkeit in Form von Protokollen und Dokumentationen erbracht werden können.

Eine große Gefahr für Personen oder Beschäftigte ist auch eine mangelhafte Datensicherheit. Erwägungsgrund 75 der DSGVO beschreibt die mit der Verarbeitung personenbezogener Daten einhergehenden Risiken und damit die Gefährdungslage durch unbefugten Zugriff wie folgt: „Die Risiken für die Rechte und Freiheiten natürlicher Personen, mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere, können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen betreffende Daten verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.“

2.2. Festlegung eines zu niedrigen Schutzbedarfs

Eine weitere Gefahr für Personen bzw. Beschäftigte ist ein falsch angesetzter Schutzbedarf ihrer personenbezogenen Daten. Dieser Schutzbedarf, der typischerweise durch die Institution, die verantwortlich personenbezogene Daten verarbeitet, selbst festgelegt wird, kann aus verschiedenen Gründen falsch oder zu niedrig angesetzt sein:

- Die Institution hat den gegenüber der Informationssicherheit erweiterten Schutzzielkatalog des Datenschutzes nicht berücksichtigt.
- Die Institution hat bei der Schutzbedarfsermittlung nicht zwischen den Risiken für die Umsetzung der Grundrechte der Betroffenen und den Risiken für die Institution unterschieden.
- Die Institution hat zwar die beiden Schutzinteressen unterschieden, aber die Funktionen des Verfahrens und der Schutzmaßnahmen zugunsten der Institution bzw. zu Ungunsten betroffener Personen gestaltet.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins CON.2 *Datenschutz* aufgeführt. Die Institutionsleitung ist dafür verantwortlich, dass die datenschutzrechtlichen Bestimmungen eingehalten werden. Die Umsetzung der zur Sicherstellung des Datenschutzes erforderlichen Maßnahmen kann sie an eine Organisationseinheit delegieren. Hiervon abzugrenzen ist die Rolle der oder des Datenschutzbeauftragten. Zu ihren Aufgaben gemäß Artikel 39 DSGVO gehört es, die Verantwortlichen, die Auftragsverarbeiter und deren jeweilige Mitarbeitende über ihre datenschutzrechtlichen Pflichten zu unterrichten und zu beraten. Ferner gehört es zu ihren Aufgaben, zu überwachen, ob die datenschutzrechtlichen Bestimmungen eingehalten werden. Die Verantwortung für die Wahrung des Datenschutzes verbleibt hingegen bei den Verantwortlichen bzw. den Auftragsverarbeitern. Der oder die Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der oder die ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Institutionsleitung
Weitere Zuständigkeiten	Datenschutzbeauftragte

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

CON.2.A1 Umsetzung Standard-Datenschutzmodell (B)

Die gesetzlichen Bestimmungen zum Datenschutz (DSGVO, BDSG, die Datenschutzgesetze der Bundesländer und gegebenenfalls einschlägige bereichsspezifische Datenschutzregelungen) MÜSSEN eingehalten werden. Wird die SDM-Methodik nicht berücksichtigt, die Maßnahmen also nicht auf der Basis der Gewährleistungsziele systematisiert und mit dem Referenzmaßnahmen-Katalog des SDM abgeglichen, SOLLTE dies begründet und dokumentiert werden.

3.2. Standard-Anforderungen

Für diesen Baustein sind keine Standard-Anforderungen definiert.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Für diesen Baustein sind keine Anforderungen für einen erhöhten Schutzbedarf definiert.

4. Weiterführende Informationen

4.1. Wissenswertes

Die EU-Datenschutz-Grundverordnung: „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)“ (DSGVO) stellt grundlegende, europaweite gesetzliche Anforderungen an die Einhaltung des Datenschutzes.

Das Standard-Datenschutzmodell (SDM) – „Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele“ des Arbeitskreises „Technik“ der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder bietet eine Methode, um gesetzliche Datenschutzvorschriften umzusetzen.



CON.3 Datensicherungskonzept

1. Beschreibung

1.1. Einleitung

Institutionen speichern immer mehr Daten und sind gleichzeitig immer stärker auf sie angewiesen. Gehen Daten verloren, z. B. durch defekte Hardware, Malware oder versehentliches Löschen, können gravierende Schäden entstehen. Dies kann klassische IT-Systeme, wie Server oder Clients betreffen. Aber auch Router, Switches oder IoT-Geräte können schützenswerte Informationen, wie Konfigurationen, speichern. Deswegen umfasst der Begriff IT-System in diesem Baustein alle Formen von IT-Komponenten, die schützenswerte Informationen speichern.

Durch regelmäßige Datensicherungen lassen sich Auswirkungen von Datenverlusten minimieren. Eine Datensicherung soll gewährleisten, dass durch einen redundanten Datenbestand der Betrieb der Informationstechnik kurzfristig wiederaufgenommen werden kann, wenn Teile des aktiv genutzten Datenbestandes verloren gehen. Das Datensicherungskonzept nimmt somit auch eine zentrale Rolle in der Notfallplanung ein. Die wesentlichen Anforderungen der Notfallplanung, wie der maximal zulässige Datenverlust (Recovery Point Objective, RPO), sollten in dem Datensicherungskonzept berücksichtigt werden.

Zu einem vollständigen Datensicherungskonzept gehört nicht nur der Aspekt, wie Datensicherungen präventiv erstellt werden (Backup), sondern auch, wie angefertigte Datensicherungen auf dem Ursprungssystem wiederhergestellt werden (Restore). Für eine Datensicherung können die unterschiedlichsten Lösungen eingesetzt werden, wie beispielsweise:

- Storage-Systeme,
- Bandlaufwerke,
- mobile Wechseldatenträger (USB-Sticks oder externe Festplatten),
- optische Datenträger sowie
- Online-Lösungen.

Diese Lösungen werden im Folgenden als Speichermedien für die Datensicherung zusammengefasst. Dem gegenüber werden Datenspiegelungen über RAID-Systeme nicht als Datensicherung verstanden, da die gespiegelten Daten simultan verändert werden. Das bedeutet, dass eine Datenspiegelung über ein RAID-System zwar einem Ausfall durch einen Hardwaredefekt einzelner Datenträger vorbeugen kann, sie kann jedoch nicht vor einem unbeabsichtigten Überschreiben oder einer Infektion mit Schadsoftware schützen.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, aufzuzeigen, wie Institutionen ein Datensicherungskonzept erstellen können und wie sie anhand dessen ihre Daten angemessen gegen einen Datenverlust absichern können.

1.3. Abgrenzung und Modellierung

Der Baustein CON.3 *Datensicherungskonzept* ist einmal auf den gesamten Informationsverbund anzuwenden.

Der Baustein beschreibt grundsätzliche Anforderungen, die zu einem angemessenen Datensicherungskonzept beitragen. Nicht behandelt werden Anforderungen an die Aufbewahrung und Erhaltung von elektronischen Dokumenten für die Langzeitspeicherung. Diese finden sich im Baustein OPS.1.2.2 *Archivierung*.

Dieser Baustein behandelt auch keine systemspezifischen und anwendungsspezifischen Eigenschaften von Datensicherungen. Die systemspezifischen und anwendungsspezifischen Anforderungen an das Datensicherungskon-

zept werden in den entsprechenden Bausteinen der Schichten NET *Netze und Kommunikation*, SYS *IT-Systeme* und APP *Anwendungen* ergänzt.

Für das Löschen und Vernichten von Datensicherungen muss der Baustein CON.6 *Löschen und Vernichten* berücksichtigt werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein CON.3 *Datensicherungskonzept* von besonderer Bedeutung.

2.1. Fehlende Datensicherung

Wenn Daten verloren gehen und sie nicht vorher gesichert wurden, kann das existenzbedrohende Folgen für eine Institution haben. Daten können z. B. durch Malware, technische Fehlfunktionen oder einen Brand verloren gehen, aber auch, wenn Mitarbeitende Daten absichtlich oder unabsichtlich löschen.

2.2. Fehlende Wiederherstellungstests

Werden Daten regelmäßig gesichert, gewährleistet dies nicht automatisch, dass diese auch problemlos wiederhergestellt werden können. Wenn nicht regelmäßig getestet wird, ob sich Daten wiederherstellen lassen, kann es sein, dass die gesicherten Daten nicht wiederhergestellt werden können.

2.3. Ungeeignete Aufbewahrung der Speichermedien für die Datensicherungen

Auf den Speichermedien für die Datensicherungen befinden sich zahlreiche schützenswerte Informationen der Institution, egal ob es sich um klassische Bänder oder moderne Storage-Systeme handelt. Werden die Speichermedien für die Datensicherungen an einem unsicheren Ort aufbewahrt, kann bei einem Angriff eventuell darauf zugegriffen und schützenswerte Informationen gestohlen oder manipuliert werden. Ebenso können Speichermedien für die Datensicherungen durch ungünstige Lagerung oder klimatische Raumbedingungen unbrauchbar werden. Dann sind die auf ihnen abgespeicherten Informationen nicht mehr verfügbar.

2.4. Fehlende oder unzureichende Dokumentation

Wenn Datensicherungsmaßnahmen und besonders die Maßnahmen zur Wiederherstellung nicht oder nur mangelhaft dokumentiert sind, kann dies die Wiederherstellung erheblich verzögern. Dadurch können sich in der Folge auch wichtige Prozesse verzögern, z. B. in der Produktion. Zudem ist es möglich, dass sich eine Datensicherung gar nicht mehr einspielen lässt und die Daten damit verloren sind.

Wenn die Information zur Wiederherstellung nur digital vorliegt, besteht die Gefahr, dass diese bei Großschäden (wie Ransomware) ebenfalls verloren geht, und die Wiederherstellung dann gefährdet ist.

2.5. Missachtung gesetzlicher Vorschriften

Wenn bei der Datensicherung gesetzliche Vorgaben, wie beispielsweise Datenschutzgesetze, nicht beachtet werden, können gegen die Institution Bußgelder verhängt oder Schadenersatzansprüche geltend gemacht werden.

2.6. Unsichere Anbieter für Online-Datensicherungen

Lagern Institutionen ihre Datensicherung online zu einer fremden Institution aus, können Angriffe auf diese auch die Daten der eigenen Institution betreffen. In der Folge kann dies dazu führen, dass schützenswerte Daten abfließen.

Des Weiteren besteht die Gefahr, dass ungünstige vertragliche Konditionen dazu führen, dass Datensicherungen nicht kurzfristig verfügbar sind. Im Notfall können sie nicht in einer definierten Zeitspanne wiederhergestellt werden.